Halasz 2000-0249

REMARKS

Claims 1-51 were rejected under 35 USC 102 as being anticipated by Ricciulli, US patent 6,816,910 ('910). Applicants respectfully traverse.

At the outset it should be pointed out that the '910 reference teaches an approach that is totally different from the approach disclosed by applicants so, not surprisingly, as demonstrated below, the subject claims are quite different from the teachings found in the '910 reference.

The '910 reference seeks to prevent success of a flooding attack by having a computer that is privy to packets that flow to and from a server that is being protected. This computer maintains a queue of SYN packets that have not been acknowledged by clients that sent the SYM packet[1], and when that queue reaches a preselected threshold and a new SYN packet arrives, the computer discards from the queue a randomly selected SYN packet having a source address that is not known to the system (FIG. 4, step 420) or SYN packets that are older than a preselected age (FIG. 5, step 530). Correspondingly the computer sends a Reset packet to the server, so that it also would discard the appropriate SYN packet from its unacknowledged SYN packets queue (steps 422 and 534).

In contradistinction, applicants disclosed a method where a determination that a flooding attack might be in progress is based on the arrival rate of packets. Thus, claim 1 specifies measuring packets inter-arrival time (i.e., arrival time of one packet compared to arrival time of another packet) and taking action when that time is below some threshold. This action is totally independent of the number of SYN packets in any unacknowledged SYN packets queue; and conversely, the '910 reference is totally independent of time.

In connection with claims 1, 13, 20, 23-24, and 31, the Examiner asserts that the '910 reference teaches the step of

---

[1] It may be helpful to mention that the connection establishment protocol is that of a first device sending a "request" message to a second device for a connection in the form of a SYN packet. The second device responds to the first device with a "synchronize" message in the form of a SYN_ACK packet, which effectively says that the second device is ready, and the first device responds to the second device with a "OK, let's go ahead" message in the form of an ACK packet.

> determining whether the first request and the second request have arrived at the host device within a predetermined time interval, the predetermined time interval being based on a probability distribution function of the arrival times of previous requests for starting data connections received at the host device from a given originating location

and that the '910 reference also teaches the step of

> denying the second data connection to the client.

in response to the step of determining. In support of the first assertion the Examiner points to col. 5, lines 1-10 of the reference, and in support of the second assertion the Examiner points to col. 5, lines 22-40. Applicants respectfully disagree.

The col. 5, lines 1-10 passage pointed to by the Examiner relative to the first assertion states:

> The computer 310 captures all, or many, TCP packets being transmitted on the network 320 to the servers 330 being protected and proactively processes the packets to avoid filling up the connection pending queue of the protected servers 330. A running total can be kept of outstanding SYN packets (SYN packets that have not yet been acknowledged by the clients 340) and a TCP reset message can be sent by the sending component to the servers 330 in order to keep the total of all outstanding SYN packets under a predetermined threshold value.

Clearly, there is no mention in the above-quoted cited passage of any predetermined time interval that is considered, nor any mention of a probability distribution of arrival times; so the Examiner's assertion fails on two counts. Indeed, there is no mention in the entirety of the '910 reference of any comparison of inter-arrival time of packets (i.e., arrival time of one packet compared to arrival time of another packet), and the only comparison that involves time is found in the second paragraph of col. 6 (lines 8-20), where the arrival time of a SYN packet, T, is compared to the current time to determine whether it's too old (in which case it is deleted). Hence, it is respectfully submitted that claims 1, 13, 20, 23-24, and 31 are not anticipated by the '910 reference.

As for the col. 5, lines 22-40 passage that was pointed to by the Examiner relative to the second assertion, it states:

> At 402, a TCP packet is read. At 404, if the packet is a SYN packet and the source (return) address is unknown, then at 406 the packet is added to the SYN packet database, and at 408 the outstanding SYN packet total is increased. If the 404 result is no, then 410 is next. At 410, if the packet is an acknowledge (ACK) message, then at 412 its

> corresponding record in the SYN packet database is deleted, at 414 the outstanding SYN packet total is decreased by one, and at 416 the client source address is recorded. Following 408, at 418, if the outstanding SYN packet total goes above a threshold 420 is next. At 420, one of the outstanding SYN records not corresponding to a known good client recorded in 416 is chosen at random. At 422, a "spoofed" TCP reset packet is sent to the server from the sending component as if the packet was coming from the client that originally sent the SYN packet. At 424, the outstanding SYN total is decremented, for example by one. At 426, the outstanding SYN record used for sending the TCP reset packet is deleted.

Clearly, this passage teaches the method as outlined by applicants above, and the only step that can be said to qualify as a step of "denying the second data connection to the client" is step 422, where "a 'spoofed' TCP reset packet is sent to the server from the sending component as if the packet was coming from the client that originally sent the SYN packet." This RESET packet causes the protected server to drop the SYN packet in its queue and, thus, perhaps it can be said that a data connection is "denied" (though some may argue that it's stretching the definition of the word "denied." However, this step is taken in response to a determination that (a) an arriving packet is a SYN packet with an unknown source address (step 404) and that (b) the outstanding SYN packet total goes above a threshold (step 418). Since the denial of service step of the reference is NOT responsive to a determination specified in the subject claims (which determination is not even undertaken by the reference), it follows that it is different from the "step of denying" specified in the subject claims. Consequently, it is respectfully submitted that claims 1, 13, 20, 23-24, and 31 are (for this reason as well) not anticipated by the '910 reference.

Claims 2, 21, and 32 specify preventing transmission of a synchronize message, and the Examiner asserts that this is taught in col. 7, lines 16-23. Applicants respectfully disagree. The passage cited by the Examiner states:

> One Internet cookie embodiment increases the capacity of storing outstanding connection pending entries, thus requiring that an attacker send a much greater number of SYN packets. This embodiment can increase the cost of an attack. The embodiment can require the server to devote more resources to prevent the SYN flooding attacks, and can be adequate to discourage attacks carried out by individuals with limited bandwidth at their disposal

Clearly this passage does teach any preventing or refraining of sending anything to the client that sent the first request (such as a SYN_ACK packet). Therefore, it is respectfully submitted that claims 2, 21, and 32 are not anticipated by the '910 reference also by virtue of the specific limitations found in claims 2, 21, and 32.

As for claims 5 and 35, the Examiner asserts that the passage at col. 5, lines 22-40 teaches the limitation of "calculating a difference value in the arrival times of the first request and second request at the host device for comparing the difference value to the predetermined time interval." Applicants respectfully disagree.

The cited passage is quoted above, and the following can be categorically said about it: (1) it does not perform any calculation of a difference; (2) it does not deal with a time of arrival of anything; and (3) it does not deal with two requests, relative to each, in any other way; and (4) it does not compare any difference to a predetermined time interval. In short, the passage cited by the Examiner does not come even close to the limitation of claims 5 and 35. Therefore, it is respectfully submitted that claims 5 and 35 are not anticipated by the '910 reference also by virtue of the limitations found in claims 5 and 35.

As for claims 6 and 36, the Examiner asserts that the passage at col. 4, lines 44-58 teaches the limitation of transmitting a signal to a network control center for taking corrective action against the client. The Examiner has not identified what the Examiner considers the "network control center." Independent of that fact, it is noted that the cited passage states:

> In some embodiment, connection pending entries when the queue is filled by SYN requests can be randomly dropped. In one embodiment, the server can replace at random one of the entries in the queue and can let the client time out and can later retry the connection with another SYN.
>
> To maximize the overall response time of a server under attack, other embodiments have the server send a RST message to the client. With this addition, if a client's SYN entry happens to be dropped by the server, the client can be notified immediately with an EOF signal at the application level. Subsequently, the client can retry the connection establishment until the connection goes through. A client can be guaranteed connection establishment under most conditions.

The only message that appears to be discussed in this passage is an EOF signal that is sent to the client that sent a SYN packet which the server chooses to drop. This is neither

a message to a "network control center" nor is it a message "against the client." Therefore, it is respectfully submitted that claims 6 and 36 are not anticipated by the '910 reference also by virtue of the limitations found in claims 6 and 36.

As for claims 7, 37, 41, and 49, Examiner asserts that the passage at col. 4, lines 44-58 teaches the limitation of

> barring the client access to the host device by downloading from the network control center appropriate commands to the server and appropriate commands to specific switching devices in the network.

Applicants respectfully disagree, because the cited passage states:

> At 514, if TCP_signal=(TCP_ACK and not TCP SYN) or TCP_RST, then 516 is next. At 516, record is found pertaining to this packet in database B. At 518, if record was found, then 520 is next. At 520, source address is added to database A. At 524, the TABLE_SIZE variable, indexed by port number and destination address, is decremented. At 524, record is deleted in database B.

This passage teaches that when an ACK packet arrives, the method adds the source address of the packet into A -- which is collection of addresses that are known to the system (and therefore, with some assurance are known to belong not to an attacker) -- and removes record corresponding to the source of the received ACK packet from B. There is no mention here of any "network control center," there is no mention of any action that could possibly be classified as barring anything from any device, there is no mention of any switching device in the network, and there is no mention of any message that can be classified as commands to switching devices. Therefore, it is respectfully submitted that claims 7, 37, 41, and 49are not anticipated by the '910 reference also by virtue of the limitations found in claims 7, 37, 41, and 49.

As for claims 8, 32, 42, 50, and 51, Examiner asserts that the passage at col. 4, lines 47-67 teaches the step of

> signaling the host device to shut down and the step of sending commands from the network control center to one or more standby servers to take over the processing functions performed by the host device that was shut down

Applicants respectfully disagree. The cited passage teaches that FIG. 3 is one embodiment for limiting connection resources. Specifically, it teaches that computer 310 (which is charged with protecting servers 330) implements an "early drop" scheme of packets. This computer does not signal the host (i.e., servers 330) to shut down, it does

not describe a "network control center," it does not describe sending commands to anything that could be considered a "network control center," and it does not send commands to any standby servers. In short, it is respectfully submitted that the cited passage teaches nothing that is specified in claims 8, 32, 42, 50, and 51 and, therefore it is believed that these claims are not anticipated by the '910 reference.

As for claims 9, 22, 39, and 43, Examiner asserts that the passage at col. 5, lines 1-18 teaches the step of

> proceeding with establishment of the second data connection if the first request and the second request have arrived at the host device outside of the predetermined time interval

Applicants respectfully disagree. The cited passage is quoted above, and from a perusal thereof it is quite clear that the passage does not address the question of whether or not a second connection should be established, it does not even address the question of establishing any connection, and time is totally absent from anything that the passage teaches, not to mention a time *interval*. Therefore, it is respectfully submitted that claims 9, 22, 39, and 43 are not anticipated by the '910 reference per force of the limitations found in the claims in addition to being not anticipated by virtue of their dependence on an unanticipated claim.

Claims 10 and 11 define subject matter that is also not taught in the passage cited by the Examiner, and moreover, these claims depend on claim 9 which, as demonstrated above, is not anticipated by the '910 reference.

As for claims 14, 25, and 45, applicants respectfully direct the Examiner's attention to the arguments above concerning claim 2.

Regarding claims 17, 28, and 48, the Examiner asserts that the passage at col. 5, lines 22-40 teaches the step of

> calculating a difference value in arrival times of the initializing request and the previously received initializing request from the originating address

Applicants disagree, and respectfully direct the Examiner's attention to the remarks made above about what is taught and not taught in the cited passage. Applicants believe, based on the above-presented arguments, that claims 17, 28, and 48 are not anticipated by the '910 reference.

Halasz 2000-0249

As for claims 18 and 29, applicants have already addressed the fact that the reference does NOT teach a "network control center" and, therefore, it is respectfully submitted that claims 18 and 19 are not anticipated by the '910 reference.

Regarding claims 19 and 20, the Examiner asserts that the passage at col. 4, lines 27-46 teaches the step of

> monitoring a plurality of data packets arriving at the host device so as to generate a probability distribution of the arrival times of a plurality of initializing requests from the originating address.

Applicants respectfully disagree. The cited passage teaches some different embodiments that can be realized. The embodiment that comes closest is the one where the embodiment learns "an optimal threshold for intervening in the defense by monitoring the average operation of the server" (col. 4, lines 34-36), but this still does not teach a focus on arrival times, and it certainly does not teach generating a probability distribution. Therefore, it is respectfully submitted that claims 19 and 20 are not anticipated by the '910 reference per force of the limitations found in the claims in addition to being not anticipated by virtue of their dependence on an unanticipated claim.

As for claims 40 and 44, the Examiner's attention is respectfully directed to the arguments presented above in connection with claims that specify arrival times, probability distribution function, or network control center. It is respectfully submitted that each of these limitations renders the subject claims unanticipated by the '910 reference.

In view of the above remarks, it is respectfully submitted that all of the Examiner's rejections have been overcome. Reconsideration and allowance are respectfully solicited.

Respectfully,
Sylvia Halasz
Kamlesh T. Tewani

Dated: 2/6/06

By _____
Henry T. Brendzel
Reg. No. 26,844
Phone (973) 467-2025
Fax (973) 467-6589
email brendzel@comcast.net